CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

NEW QUESTION 1
Due to budget constraints, an organization created a policy that only permits vulnerabilities rated high and critical according to CVSS to be fixed or mitigated. A security analyst notices that many vulnerabilities that were previously scored as medium are now breaching higher thresholds. Upon further investigation, the analyst notices certain ratings are not aligned with the approved system categorization. Which of the following can the analyst do to get a better picture of the risk while adhering to the organization's policy?

A. Align the exploitability metrics to the predetermined system categorization.
B. Align the remediation levels to the predetermined system categorization.
C. Align the impact subscore requirements to the predetermined system categorization.
D. Align the attack vectors to the predetermined system categorization.

Answer: C

Explanation:
Aligning the impact subscore requirements to the predetermined system categorization can help the analyst get a better picture of the risk while adhering to the organization’s policy. The impact subscore is one of the components of the CVSS base score, which reflects the severity of a vulnerability. The impact subscore is calculated based on three metrics: confidentiality, integrity, and availability. These metrics can be adjusted according to the system categorization, which defines the security objectives and requirements for a system based on its potential impact on an organization’s operations and assets. By aligning the impact subscore requirements to the system categorization, the analyst can ensure that the CVSS scores reflect the true impact of a vulnerability on a specific system and prioritize remediation accordingly.

NEW QUESTION 2
A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.
Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

A. Designing data protection schemes to mitigate the risk of loss due to multitenancy
B. Implementing redundant stores and services across diverse CSPs for high availability
C. Emulating OS and hardware architectures to blur operations from CSP view
D. Purchasing managed FIM services to alert on detected modifications to covered data

Answer: A

NEW QUESTION 3
An administrator at a software development company would like to protect the integrity Of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted CA. Which of the following is MOST likely the cause of the signature failing?

A. The NTP server is set incorrectly for the developers.
B. The CA has included the certificate in its CRL_
C. The certificate is set for the wrong key usage.
D. Each application is missing a SAN or wildcard entry on the certificate.

Answer: C

Explanation:
Digital signatures require the use of a cryptographic key pair, which consists
of a private key used to sign the application and a public key used to verify the signature. If the certificate used for signing the application is set for the wrong key usage, then the signature will fail. This can happen if the certificate is set for encrypting data instead of signing data, or if the certificate is set for the wrong algorithm, such as using an RSA key for an ECDSA signature.

NEW QUESTION 4
A company Invested a total of $10 million lor a new storage solution Installed across live on-site datacenters. Fitly percent of the cost of this Investment was for solid-state storage.
Due to the high rate of wear on this storage, the company Is estimating that 5% will need to be replaced per year. Which of the following is the ALE due to storage replacement?

A. $50,000
B. $125,000
C. $250,000
D. $500.000
E. $51,000,000

Answer: C

NEW QUESTION 5
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user’s workstation:
graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?

A. NX bit
B. ASLR
C. DEP
D. HSM

Answer: B

Explanation:
https://eklitzke.org/memory-protection-and-aslr
ASLR (Address Space Layout Randomization) is a technology that can mitigate the manipulation of memory segments caused by a buffer overflow attack. ASLR randomizes the location of memory segments, such as the stack, heap, or libraries, making it harder for an attacker to predict or control where to inject malicious code or overwrite memory segments. NX bit (No-eXecute bit) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. NX bit marks certain memory segments as non-executable, preventing an attacker from running code in those segments. DEP (Data Execution Prevention) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. DEP uses hardware and software mechanisms to mark certain memory regions as data-only, preventing an attacker from running code in those regions. HSM (Hardware Security Module) is a device that can provide cryptographic functions and key storage, but it does not mitigate the manipulation of memory segments
caused by a buffer overflow attack. Verified References: https://www.comptia.org/blog/what-is-aslr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 6
A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

A. Inherent
B. Low
C. Mitigated
D. Residual.
E. Transferred

Answer: D

NEW QUESTION 7
A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.
Which of the following BEST describes the type of malware the solution should protect against?

A. Worm
B. Logic bomb
C. Fileless
D. Rootkit

Answer: C

Explanation:
Reference: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital- threats/tracking-detecting-and-thwarting-powershell-based-malware-and-attacks

NEW QUESTION 8
A municipal department receives telemetry data from a third-party provider The server collecting telemetry sits in the municipal departments screened network and accepts connections from the third party over HTTPS. The daemon has a code execution vulnerability from a lack of input sanitization of out-of-bound messages, and therefore, the cybersecurity engineers would like to Implement nsk mitigations. Which of the following actions, if combined, would BEST prevent exploitation of this vulnerability? (Select TWO).

A. Implementing a TLS inspection proxy on-path to enable monitoring and policy enforcement
B. Creating a Linux namespace on the telemetry server and adding to it the servicing HTTP daemon
C. Installing and configuring filesystem integrity monitoring service on the telemetry server
D. Implementing an EDR and alert on Identified privilege escalation attempts to the SIEM
E. Subscribing to a UTM service that enforces privacy controls between the internal network and the screened subnet
F. Using the published data schema to monitor and block off nominal telemetry messages

Answer: AC

Explanation:
A TLS inspection proxy can be used to monitor and enforce policy on HTTPS connections, ensuring that only valid traffic is allowed through and malicious traffic is blocked. Additionally, a filesystem integrity monitoring service can be installed and
configured on the telemetry server to monitor for any changes to the filesystem, allowing any malicious changes to be detected and blocked.

NEW QUESTION 9
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<ENTITY xxe SYSTEM "file:///etc/password">]>
<doc>&xxe;</doc>
```

Which of the following would BEST mitigate this vulnerability?

A. CAPTCHA
B. Input validation
C. Data encoding
D. Network intrusion prevention

Answer: B

Explanation:
Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe

NEW QUESTION 10
To save time, a company that is developing a new VPN solution has decided to use the OpenSSL library within Its proprietary software. Which of the following should the company consider to maximize risk reduction from vulnerabilities introduced by OpenSSL?

A. Include stable, long-term releases of third-party libraries instead of using newer versions.
B. Ensure the third-party library implements the TLS and disable weak ciphers.
C. Compile third-party libraries into the main code statically instead of using dynamic loading.
D. Implement an ongoing, third-party software and library review and regression testing.

Answer: D

Explanation:
Implementing an ongoing, third-party software and library review and regression testing is the best way to maximize risk reduction from vulnerabilities introduced by OpenSSL. Third-party software and libraries are often used by developers to save time and resources, but they may also introduce security risks if they are not properly maintained and updated. By reviewing and testing the third-party software and library regularly, the company can ensure that they are using the latest and most secure version of OpenSSL, and that their proprietary software is compatible and functional with it. References: [CompTIA CASP+ Study Guide, Second Edition, page 362]

NEW QUESTION 11
A security architect is given the following requirements to secure a rapidly changing enterprise with an increasingly distributed and remote workforce
• Cloud-delivered services
• Full network security stack
• SaaS application security management
• Minimal latency for an optimal user experience
• Integration with the cloud 1AM platform Which of the following is the BEST solution?

A. Routing and Remote Access Service (RRAS)
B. NGFW
C. Managed Security Service Provider (MSSP)
D. SASE

Answer: D

NEW QUESTION 12
A security analyst sees that a hacker has discovered some keys and they are being made
available on a public website. The security analyst is then able to successfully decrypt the data using the keys from the website. Which of the following should the security analyst recommend to protect the affected data?

A. Key rotation
B. Key revocation
C. Key escrow
D. Zeroization
E. Cryptographic obfuscation

Answer: E

NEW QUESTION 13
A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.
Which of the following is a security concern that will MOST likely need to be addressed during migration?

A. Latency
B. Data exposure
C. Data loss
D. Data dispersion

Answer: B

Explanation:
Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but a availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or control of data. Verified References: https://www.comptia.org/blog/what-is-data-exposure
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 14
A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented in order to meet contractual requirements, the company must achieve the following thresholds
• 99 99% uptime
• Load time in 3 seconds
• Response time = <1 0 seconds
Starting with the computing environment, which of the following should a security engineer recommend to BEST meet the requirements? (Select THREE)

A. Installing a firewall at corporate headquarters
B. Deploying a content delivery network
C. Implementing server clusters
D. Employing bare-metal loading of applications
E. Lowering storage input/output
F. Implementing RAID on the backup servers
G. Utilizing redundant power for all developer workstations
H. Ensuring technological diversity on critical servers

Answer: BCE

Explanation:
To meet the contractual requirements of the web service provider, a security engineer should recommend the following actions:
? Deploying a content delivery network (CDN): A CDN is a distributed system of
servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the uptime, load time, and response time of web services by caching content closer to the users, reducing latency and bandwidth consumption. A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the web service availability12.
? Implementing server clusters: A server cluster is a group of servers that work
together to provide high availability, scalability, and load balancing for web services. A server cluster can help improve the uptime, load time, and response time of web services by distributing the workload across multiple servers, reducing the risk of single points of failure and performance bottlenecks. A server cluster can also help recover from failures by automatically switching to another server in case of a malfunction34.
? Lowering storage input/output (I/O): Storage I/O is the amount of data that can be
read from or written to a storage device in a given time. Storage I/O can affect the performance of web services by limiting the speed of data transfer between the servers and the storage devices. Lowering storage I/O can help improve the load time and response time of web services by reducing the latency and congestion of data access. Lowering storage I/O can be achieved by using faster storage devices, such as solid-state drives (SSDs), optimizing the storage layout and configuration, such as using RAID or striping, and caching frequently accessed data in memory5 .
Installing a firewall at corporate headquarters is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can help improve the security of web services by preventing unauthorized access and attacks, but it may also introduce additional latency and complexity to the network.
Employing bare-metal loading of applications is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Bare-metal loading is a technique that allows applications to run directly on hardware without an operating system or a hypervisor. Bare-metal loading can help improve the performance and efficiency of applications by eliminating the overhead and interference of other software layers, but it may also increase the difficulty and cost of deployment and maintenance.
Implementing RAID on the backup servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. RAID (redundant array of independent disks) is a technique that combines multiple disks into a logical unit that provides improved performance, reliability, or both. RAID can help improve the availability and security of backup data by protecting it from disk failures or corruption, but it may also introduce additional complexity and overhead to the backup process.
Utilizing redundant power for all developer workstations is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Redundant power is a technique that provides multiple sources of power for an IT system in case one fails. Redundant power can help improve the availability and reliability of developer workstations by preventing them from losing power due to outages or surges, but it may also increase the cost and energy consumption of the system.
Ensuring technological diversity on critical servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Technological diversity is a technique that uses different types of hardware, software, or platforms in an IT environment. Technological diversity can help improve resilience by reducing single points of failure and increasing compatibility, but it may also introduce additional complexity and inconsistency to the
environment. References: What Is CDN? How Does CDN Work? | Imperva, What Is Server Clustering? | IBM, What Is Server Clustering? | IBM, Server Clustering: What It Is & How It Works | Liquid Web, Storage I/O Performance - an overview | ScienceDirect Topics, [How
to Improve Storage I/O Performance | StarWind Blog], [What Is Firewall Security? | Cisco], [What is Bare Metal? | IBM], [What is RAID? | Dell Technologies US], [What Is Redundant Power Supply? | Dell Technologies US], [Technological Diversity - an overview | ScienceDirect Topics]

NEW QUESTION 15
A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:
Unauthorized insertions into application development environments
Authorized insiders making unauthorized changes to environment configurations
Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

A. Perform static code analysis of committed code and generate summary reports.
B. Implement an XML gateway and monitor for policy violations.
C. Monitor dependency management tools and report on susceptible third-party libraries.
D. Install an IDS on the development subnet and passively monitor for vulnerable services.
E. Model user behavior and monitor for deviations from normal.
F. Continuously monitor code commits to repositories and generate summary logs.

Answer: EF

Explanation:
Modeling user behavior and monitoring for deviations from normal and continuously monitoring code commits to repositories and generating summary logs are actions that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations. Modeling user behavior and monitoring for deviations from normal is a technique that uses baselines, analytics, machine learning, or other methods to establish normal patterns of user activity and identify anomalies or outliers that could indicate malicious or suspicious behavior. Modeling user behavior and monitoring for deviations from normal can help detect unauthorized insertions into application development environments, as it can alert on unusual or unauthorized access attempts, commands, actions, or transactions by users. Continuously monitoring code commits to repositories and generating summary logs is a technique that uses tools, scripts, automation, or other methods to track and record changes made to code repositories by developers, testers, reviewers, or other parties involved in the software development process. Continuously monitoring code commits to repositories and generating summary logs can help detect authorized insiders making unauthorized changes to environment configurations, as it can audit and verify the source, time, reason, and impact of code changes made by authorized users. Performing static code analysis of committed code and generate summary reports is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to detect vulnerabilities, errors, bugs, or quality issues in committed code. Implementing an XML gateway and monitor for policy violations is not an action that will enable the data feeds needed to detect

unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to protect XML-based web services from threats or attacks by validating XML messages against predefined policies. Monitoring dependency management tools and report on susceptible third-party libraries is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to identify outdated or vulnerable third-party libraries used in software development projects. Installing an IDS (intrusion detection system) on the development subnet and passively monitor for vulnerable services is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes

NEW QUESTION 16
A Chief Security Officer (CSO) is concerned about the number of successful ransomware attacks that have hit the company. The data Indicates most of the attacks came through a
fake email. The company has added training, and the CSO now wants to evaluate whether the training has been successful. Which of the following should the CSO implement?

A. Simulating a spam campaign
B. Conducting a sanctioned vishing attack
C. Performing a risk assessment
D. Executing a penetration test

Answer: A

Explanation:
A spam campaign is a mass distribution of unsolicited or fraudulent emails that may contain malicious links, attachments, or requests. Spam campaigns are often used by attackers to deliver ransomware, which is a type of malware that encrypts the victim's data and demands a ransom for its decryption.
Simulating a spam campaign would allow the Chief Security Officer (CSO) to evaluate whether the training has been successful in reducing the number of successful ransomware attacks that have hit the company, because it would:
? Test the employees' ability to recognize and avoid clicking on fake or malicious
emails, which is one of the main vectors for ransomware infection.
? Measure the effectiveness of the training by comparing the click-through rate and the infection rate before and after the training.
? Provide feedback and reinforcement to the employees by informing them of their performance and reminding them of the best practices for email security.

NEW QUESTION 17
A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.
Which of the following is the BEST solution to meet these objectives?

A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: B

Explanation:
PAM (Privileged Access Management) is a solution that can increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. By implementing PAM, removing users from the local administrators group, and prompting users for explicit approval when elevated privileges are required, the security engineer can reduce the attack surface, prevent unauthorized access, and enforce the principle of least privilege. Implementing PAM, keeping users in the local administrators group, and enabling local administrator account monitoring may not provide enough control or visibility over local administrator accounts, as users could still abuse or compromise their privileges. Implementing EDR (Endpoint Detection and Response) may not provide enough control or visibility over local administrator accounts, as EDR is mainly focused on detecting and responding to threats, not managing privileges. Enabling user behavior analytics may not provide enough control or visibility over local administrator accounts, as user behavior analytics is mainly focused on identifying anomalies or risks in user activity, not managing privileges. Verified References: https://www.comptia.org/blog/what-is-pam
https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 18
A managed security provider (MSP) is engaging with a customer who was working through a complete digital transformation Part of this transformation involves a move to cloud servers to ensure a scalable, high-performance, online user experience The current architecture includes:
• Directory servers
• Web servers
• Database servers
• Load balancers
• Cloud-native VPN concentrator
• Remote access server
The MSP must secure this environment similarly to the infrastructure on premises Which of the following should the MSP put in place to BEST meet this objective? (Select THREE)

A. Content delivery network
B. Virtual next-generation firewall
C. Web application firewall
D. Software-defined WAN
E. External vulnerability scans
F. Containers
G. Microsegmentation

Answer: BCG

Explanation:
A virtual next-generation firewall (vNGFW) is a software version of a NGFW that can be deployed on cloud servers to provide advanced network security features. A vNGFW can help secure the cloud environment similarly to the infrastructure on premises by providing functions such as URL filtering, SSL/TLS inspection, deep

packet inspection, antivirus, IPS, application control, and sandboxing. A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can help secure the web servers in the cloud environment by protecting them from common attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Microsegmentation is a technique that divides a network into smaller segments or zones based on criteria such as identity, role, or function. Microsegmentation can help secure the cloud environment by isolating different types of servers and applying granular security policies to each segment.
A content delivery network (CDN) is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the availability and performance of web applications by caching content closer to the users, reducing latency and bandwidth consumption. However, a CDN does not provide the same level of security as a vNGFW or a WAF. Software-defined WAN (SD-WAN) is a technology that uses software to manage the connectivity and routing of wide area network (WAN) traffic across multiple links or carriers. SD-WAN can help improve the reliability and efficiency of WAN connections by
dynamically selecting the best path for each application based on factors such as bandwidth, latency, cost, and quality of service (QoS). However, SD-WAN does not provide the same level of security as a vNGFW or a WAF. External vulnerability scans are assessments that identify and report on the vulnerabilities and weaknesses of an IT system from an external perspective. External vulnerability scans can help improve the security posture of an IT system by providing visibility into its exposure to potential threats. However, external vulnerability scans do not provide the same level of protection as a vNGFW or a WAF. Containers are units of software that package an application and its dependencies into a standardized format that can run on any platform or environment. Containers can help improve the portability and scalability of applications by allowing them to run independently from the underlying infrastructure. However, containers do not provide the same level of security as microsegmentation. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

NEW QUESTION 19
A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?

A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.
B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Answer: A

NEW QUESTION 20
A developer implement the following code snippet.

```
catch (Exception e)
{
    if(log.isDebugEnabled())
    {
        log.debug("Caught InvalidDNDException Exception --"
        + e.toString());
    }
}
```

Which of the following vulnerabilities does the code snippet resolve?

A. SQL inject
B. Buffer overflow
C. Missing session limit
D. Information leakage

Answer: A

Explanation:
SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL commands on a database by inserting them into an input field. The code snippet resolves this vulnerability by using parameterized queries, which prevent the input from being interpreted as part of the SQL command. Verified References:
https://www.comptia.org/training/books/casp-cas-004-study-guide , https://owasp.org/www- community/attacks/SQL_Injection

NEW QUESTION 21
A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.
B. Implement the SDLC security guidelines.
C. Track the library versions and monitor the CVE website for related vulnerabilities.
D. Perform unit testing of the open-source libraries.

Answer: C

Explanation:
Reference: https://www.whitesourcesoftware.com/resources/blog/application-security-best- practices/
Tracking the library versions and monitoring the CVE (Common Vulnerabilities and Exposures) website for related vulnerabilities is an activity that the organization should incorporate into the SDLC (software development life cycle) to ensure the security of the open-source libraries integrated into its software. Tracking the library versions can help identify outdated or unsupported libraries that may contain vulnerabilities or bugs. Monitoring the CVE website can help discover publicly known vulnerabilities in the open- source libraries and their severity ratings. Performing additional SAST/DAST (static application security testing/dynamic application security testing) on the open-source libraries may not be feasible or effective for ensuring their security, as SAST/DAST are mainly focused on testing the source code or functionality of the software, not the libraries. Implementing the SDLC security guidelines is a general activity that the organization should follow

for developing secure software, but it does not specifically address the security of the open-source libraries. Performing unit testing of the open-source libraries may not be feasible or effective for ensuring their security, as unit testing is mainly focused on testing the individual components or modules of the software, not the libraries. Verified References: https://www.comptia.org/blog/what-is-cve https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 22
A major broadcasting company that requires continuous availability to streaming content needs to be resilient against DDoS attacks Which of the following is the MOST important infrastructure security design element to prevent an outage7

A. Supporting heterogeneous architecture
B. Leveraging content delivery network across multiple regions
C. Ensuring cloud autoscaling is in place
D. Scaling horizontally to handle increases in traffic

Answer: B

Explanation:
A content delivery network (CDN) is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the availability and performance of web applications by caching content closer to the users, reducing latency and bandwidth consumption. A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the application availability. Supporting heterogeneous architecture means using different types of hardware, software, or platforms in an IT environment. This can help improve resilience by reducing single points of failure and increasing compatibility, but it does not directly prevent DDoS attacks. Ensuring cloud autoscaling is in place means using cloud services that automatically adjust the amount of resources allocated to an application based on the demand or load. This can help improve scalability and performance by providing more resources when needed, but it does not directly prevent
DDoS attacks. Scaling horizontally means adding more servers or nodes to an IT environment to increase its capacity or throughput. This can help improve scalability and performance by distributing the load across multiple servers, but it does not directly prevent DDoS attacks. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.4: Select controls based on systems security evaluation models

NEW QUESTION 23
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.
Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.
B. Change the operating system.
C. Buy a new server and create an active-active cluster.
D. Upgrade the server with a new one.

Answer: A

Explanation:
Moving the server to a cloud provider is the most cost-effective solution to avoid performance issues caused by too many connections during peak seasons, such as holidays. Moving the server to a cloud provider can provide scalability, elasticity, and availability for the web server, as it can adjust its resources and capacity according to the demand and traffic. Moving the server to a cloud provider can also reduce operational and maintenance costs, as the cloud provider can handle the infrastructure and security aspects. Changing the operating system may not help avoid performance issues, as it could introduce compatibility or functionality problems, and it may not address the resource or capacity limitations. Buying a new server and creating an active-active cluster may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as complex configuration and management tasks. Upgrading the server with a new one may help avoid performance issues, but it may not be cost- effective, as it could involve hardware and software expenses, as well as migration and testing efforts. Verified References: https://www.comptia.org/blog/what-is-cloud-computing https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 24
A company launched a new service and created a landing page within its website network for users to access the service. Per company policy, all websites must utilize encryption for any authentication pages. A junior network administrator proceeded to use an outdated procedure to order new certificates. Afterward, customers are reporting the following error when accessing a new web page: NET:ERR_CERT_COMMON_NAME_INVALID. Which of the following BEST describes what the administrator should do NEXT?

A. Request a new certificate with the correct subject alternative name that includes the new websites.
B. Request a new certificate with the correct organizational unit for the company's website.
C. Request a new certificate with a stronger encryption strength and the latest cipher suite.
D. Request a new certificate with the same information but including the old certificate on the CRL.

Answer: D

NEW QUESTION 25
A user experiences an HTTPS connection error when trying to access an Internet banking website from a corporate laptop. The user then opens a browser on a mobile phone and is able to access the same Internet banking website without issue. Which of the following security configurations is MOST likely the cause of the error?

A. HSTS
B. TLS 1.2
C. Certificate pinning
D. Client authentication

Answer: A

NEW QUESTION 26
A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:
https://i.postimg.cc/8P9sB3zx/image.png
The credentials used to publish production software to the container registry should be
stored in a secure location.
Access should be restricted to the pipeline service account, without the ability for the third- party developer to read the credentials directly.
Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

A. TPM
B. Local secure password file
C. MFA
D. Key vault

Answer: D

Explanation:
Reference: https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals
A key vault is a service that provides secure storage and management of keys, secrets, and certificates. It can be used to store credentials used to publish production software to the container registry in a secure location, and restrict access to the pipeline service account without allowing the third-party developer to read the credentials directly. A TPM (trusted platform module) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing shared credentials. A local secure password file is a file that stores passwords in an encrypted format, but it is not as secure or scalable as a key vault. MFA (multi-factor authentication) is a method of verifying the identity of a user or device by requiring two or more factors, but it does not store credentials. Verified References: https://www.comptia.org/blog/what-is-a-key-vault https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 27
A company wants to quantify and communicate the effectiveness of its security controls but must establish measures. Which of the following is MOST likely to be included in an effective assessment roadmap for these controls?

A. Create a change management process.
B. Establish key performance indicators.
C. Create an integrated master schedule.
D. Develop a communication plan.
E. Perform a security control assessment.

Answer: C

NEW QUESTION 28
A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:
Work at the application layer
Send alerts on attacks from both privileged and malicious users Have a very low false positive
Which of the following should the architect recommend?

A. FIM
B. WAF
C. NIPS
D. DAM
E. UTM

Answer: D

NEW QUESTION 29
The analyst should implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics. This approach would allow the analyst to test each solution individually and measure its effectiveness against the attack, without affecting the other solutions or the production environment. This would also minimize the downtime required to implement the best solution, as only one change would be needed. The other options would either involve implementing multiple solutions at once, which could cause conflicts or errors, or collecting metrics before running the attack simulation, which would not reflect the actual impact of the solutions.
Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?

A. E-discovery
B. Review analysis
C. Information governance
D. Chain of custody

Answer: A

Explanation:
The process that involves searching and collecting evidence during an investigation or lawsuit is e-discovery. E-discovery stands for electronic discovery, which is the process of identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant to a legal matter. E-discovery can be used for civil litigation, criminal prosecution, regulatory compliance, internal investigations, and other purposes. E-discovery can help parties obtain evidence from various sources, such as emails, documents, databases, social media, cloud services, mobile devices, and others. Verified References:

- https://www.techtarget.com/searchsecurity/definition/electronic-discovery
- https://www.edrm.net/frameworks-and-standards/edrm-model/
- https://www.law.cornell.edu/wex/electronic_discovery_(federal)

NEW QUESTION 30
The Chief Information Security Officer (CISO) asked a security manager to set up a system that sends an alert whenever a mobile device enters a sensitive area of

the company's data center. The CISO would also like to be able to alert the individual who is entering the area that the access was logged and monitored. Which of the following would meet these requirements?

A. Near-field communication
B. Short Message Service
C. Geofencing
D. Bluetooth

Answer: C

Explanation:

Geofencing is a location-based service that allows an organization to define and enforce a virtual boundary around a sensitive area, such as a data center. Geofencing can use various technologies, such as GPS, Wi-Fi, cellular data, or RFID, to detect when a mobile device enters or exits the geofence. Geofencing can also trigger certain actions or notifications based on the device's location. For example, the organization can set up a geofencing policy that sends an alert to the CISO and the device user when a mobile device enters the data center area. Geofencing can also be used to restrict access to certain apps or features based on the device's location. Verified References:
? https://developer.android.com/training/location/geofencing
? https://www.manageengine.com/mobile-device-management/mdm- geofencing.html
? https://www.koombea.com/blog/mobile-geofencing/

NEW QUESTION 31
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CAS-004 Practice Exam Features:

* CAS-004 Questions and Answers Updated Frequently

* CAS-004 Practice Questions Verified by Expert Senior Certified Staff

* CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year